United States v. Shacar
21-cr-30028-MGM
EXHIBIT “1”

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	Docket No. 20-cr-10012-IT
	)	
v.	)	***LEAVE TO FILE REDACTED MEMO & EXHIBITS A-G, I-J UNDER SEAL GRANTED ON 12/27/21***
	)	
	)	
PAUL BATEMAN	)	

MOTION TO SUPPRESS EVIDENCE

The defendant, Paul Bateman, pursuant to Fed. R. Crim. P. 12 and the Fourth Amendment, respectfully moves this Court to suppress all evidence and illegal fruits obtained pursuant to the invalid search warrant issued in this case because the warrant was not supported by probable cause. Mr. Bateman also moves for a *Franks* hearing, as the affiant made material misstatements that were necessary to a finding of probable cause and omissions that, if included in the affidavit, would have vitiated probable cause.

STATEMENT OF FACTS[1]

I. The Search Warrant

On December 11, 2019, Homeland Security Investigations ("HSI") Special Agent Gregory Squire submitted an application for a search warrant to the U.S. District Court of Massachusetts. *See* Search Warrant Affidavit (attached as Exhibit A). Agent Squire sought authorization to search Mr. Bateman's home located in Bridgewater, Massachusetts for evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) and (b)(1) (Attempted Receipt of Child Pornography) and 2252A(a)(5)(B) and (b)(2) (Access with Intent to View and Possession of Child Pornography, and attempt). Ex. A at ¶ 4.

[1] The facts in this section are drawn from the discovery provided by the government. By repeating the facts here, Mr. Bateman does not adopt them as true.

The affidavit submitted in support of the search warrant contains just one allegation of criminal activity. Specifically, Agent Squire stated:

> In the course of this investigation, a foreign law enforcement agency (hereinafter, "FLA") known to U.S. law enforcement and with a history of providing reliable, accurate information in the past, notified U.S. law enforcement that FLA had determined that on April 30, 2019 at 10:38:18 UTC, IP address 73.142.30.140 was used to access online child sexual abuse and exploitation material via a website.

Id. at ¶ 23. Agent Squire went on to state that "[a]ccording to the FLA, the website had an explicit focus on the facilitation of sharing child abuse materials (images, links and videos), emphasis on BDSM, hurtcore, gore and death-related material including that of children." *Id*. He noted that "[u]sers were required to create an account (username and password) in order to access the majority of the material." *Id*. Furthermore, he stated that the "FLA provided further documentation naming the site…as Website A".[2] *Id*. The affidavit did not include any allegations that the IP address was used to create an account on the website in question. Nor did it include any information about what material was allegedly "accessed" or what section of the website the internet user associated with that IP address had visited.

Agent Squire claimed that Website A was a "child pornography online bulletin board dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children" that operated from around September 2016 to June 2019. *Id*. at ¶ 14-15. Noticeably absent from the affidavit, but ultimately disclosed by the government and otherwise known from cases arising out of the same investigation, is that Website A's operation ceased in June 2019, when its server was seized by an as-yet-unidentified FLA.[3]

---

[2] Agent Squire noted in the affidavit that the FLA "referred to the site by its actual name, not the pseudonym [Website A] used for the purposes of this warrant." Ex. A at ¶ 23, fn. 7. The government has since disclosed that the website was called [redacted]

[3] *See e.g. United States v. Kiejzo*, 4:20-cr-40036-TSH, D.E. 117-1 at pg. 3 (D. Mass. Oct. 19, 2021). The government in the instant case confirmed that both the instant case and *Kiejzo* arose out of the same

Agent Squire explained that Website A was a "hidden service" website that operated on the Tor network, a free and legal computer network "available to internet users that is designed specifically to facilitate anonymous communication over the internet." *Id*. at ¶ 6, 11. Agent Squire also included a description of how the Tor network operates and how information is anonymized on the network. *Id*. at ¶ 7-13. Specifically, Agent Squire noted that "the Tor network attempts to [facilitate anonymous communication over the internet] by routing Tor user communications through a globally distributed network of intermediary computers, or relays, along a randomly assigned path known as a 'circuit.'" *Id*. at ¶ 6. Agent Squire acknowledged that because of this process, "traditional IP address-based identification techniques are not effective." *Id*.

In the section of the affidavit discussing the tip, Agent Squire claimed that the FLA advised "that it had obtained that information through independent investigation that was lawfully authorized in FLA's country pursuant to its national laws." *Id*. at ¶ 25. In a footnote, Agent Squire averred that the FLA (since identified as the [redacted]) was a "national law enforcement agency of a country with an established rule of law" and that there was a "long history of U.S. law enforcement sharing criminal information with FLA and FLA sharing criminal investigation information with U.S. law enforcement." *Id*. at ¶ 23, fn. 6. He further noted that the FLA had "advised U.S. law enforcement that FLA had not interfered with, accessed, search or seized any data from any computer in the United States in order to obtain that IP address information." *Id*. at ¶ 25. He averred that "U.S. law enforcement did not participate in the investigative work through which FLA identified the IP address." *Id*. Finally, Agent Squire alleged that prior tips provided by the FLA had "(1) led to the identification and arrest of a U.S.-

investigation, and also confirmed via email in December 2021 after specific inquiry that there was another, separate FLA local to the server host country that conducted the seizure of Website A's server – an FLA distinct from the tip-providing FLA referenced throughout Agent Squire's affidavit.

based child pornography producer and hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse; (2) led to the seizure of evidence of child pornography trafficking and possession; and (3) been determined through further investigation to be related to targets that U.S. law enforcement investigation had independently determined were associated with child pornography trafficking and possession." *Id*. at ¶ 26. Again, these averments were only made with respect to the tip-providing FLA, as there was no such mention or averment made as to the as-yet-unidentified FLA that seized the server.

According to the affidavit, the only thing that U.S. law enforcement did in response to the tip from the FLA was to send a subpoena to Comcast Communications for subscriber information related to the IP address. *Id*. at ¶ 27. Comcast provided law enforcement with a physical address – [redacted] – associated with the IP address. *Id*. Agent Squire, after reviewing commercial databases, property records, and RMV records, indicated that Mr. Bateman owned a condo at that address and that he resided there with an adult female. *Id*. at ¶ 28-29. Agent Squire also noted that on December 10, 2019, an HSI Task Force officer conducted surveillance on the condo and observed the cars at the residence that were registered to Mr. Bateman and the woman who allegedly lived with him. *Id*. at 29-30.

A search warrant to search Mr. Bateman's home was issued on December 11, 2019. *See* Search Warrant (attached as Exhibit C). The warrant was executed the next day. Based on the evidence discovered at Mr. Bateman's home, Mr. Bateman was arrested and a complaint was filed alleging violations of 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B) (receipt and possession of child pornography). On January 16, 2020, Mr. Bateman was charged via indictment with one count of receipt of child pornography and one count of possession of child pornography.

II. Information Recently Disclosed by the Government

On December 20, 2021, in response to a specific request by the defense, the government disclosed to defense counsel that the FLA that provided the tip to U.S. law enforcement (now known to be the [redacted]) and the FLA that seized the server that hosted Website A were not just different FLAs, but from different countries altogether. The government further disclosed that the FLA that seized the server was local to the server host country (not [redacted]). The government has declined to identify the second FLA or the server host country. None of this information was included in Agent Squire's affidavit.

ARGUMENT

I. The Warrant Was Not Supported By Probable Cause.

The Fourth Amendment of the United States Constitution guarantees the right to be secure against "unreasonable searches and seizures" and requires that no warrants issue "but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched." U.S. Const. Am. IV. "With limited exceptions, it requires police officers to secure a search warrant supported by probable cause prior to effecting a search or seizure." *United States v. Gifford*, 727 F.3d 92, 98 (1st Cir. 2013).

Probable cause to issue a search warrant exists when "given all the circumstances set forth in the affidavit … there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238-39 (1983). "Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others." *Id*. at 239. This Court is tasked with "ensur[ing] that the magistrate had a substantial basis for ... concluding that probable cause existed." *Id*. at 238-39.

When an affidavit relies on information provided by a confidential informant, "the affidavit must provide some information from which a magistrate can credit the informant's credibility." *Gifford*, 727 F.3d at 99. The First Circuit applies the following non-exhaustive factors in assessing probable cause:

> (1) whether the affidavit establishes the probable veracity and basis of knowledge of persons supplying hearsay information; (2) whether an informant's statements reflect first-hand knowledge; (3) whether some or all of the informant's factual statements were corroborated wherever reasonable or practicable (e.g., through police surveillance); and (4) whether a law enforcement affiant assessed, from his professional standpoint, experience, and expertise, the probable significance of the informant's provided information.

United States v. Tiem Trinh, 665 F.3d 1, 10 (1st Cir. 2011).

Here, the affidavit submitted in support of the search warrant failed to establish a "fair probability" that evidence of a crime would be found in Mr. Bateman's home. *Gates*, 462 U.S. at 238-39. The affidavit relied entirely on one unsubstantiated and stale allegation of criminal activity by an unidentified foreign law enforcement agency. The affidavit failed to include any information as to how the FLA came across that information, how reliable the method the FLA used to obtain the information was, and whether the IP address was obtained through first-hand knowledge or through other sources. Without more information about the source of the FLA's tip and without additional corroboration, the months-old tip was not sufficient to establish probable cause, and Agent Squire could not possibly have assessed the probable significance of the tip.

a. The Tip Was Insufficient To Establish Probable Cause.

The factors outlined by the First Circuit in *Tiem Trinh*, 665 F.3d at 10, are instructive in this case because the tip that forms the entire basis of probable cause in the affidavit came from a confidential source akin to an informant. Those factors, although non-exhaustive, weigh in Mr. Bateman's favor. Agent Squire's affidavit is deficient because 1) it fails to establish the basis of

knowledge for the tip and whether it was obtained through first-hand knowledge or through hearsay (factors 1 and 2 in the *Tiem Trinh* analysis), and 2) it reflects no attempts from any U.S. law enforcement agency to corroborate the tip from the unidentified FLA (factor 3 of *Tiem Trinh*).

i. The Affidavit Fails to Establish the Basis of Knowledge for the Tip.

The affidavit is deficient because it failed to establish the basis of knowledge for the tip in two respects. First, Agent Squire did not include any information about whether the tip was obtained through first-hand knowledge or through hearsay. Second, Agent Squire included no facts about the method used to obtain the IP address information and whether that method was reliable.

The only information provided in the affidavit that offered any clues about the source of the FLA's tip were Agent Squire's statements that the FLA "had obtained [the information in the tip] through independent investigation that was lawfully authorized in FLA's country pursuant to its national laws," and that "FLA had not interfered with, accessed, searched, or seized any data from any computer in the United States in order to obtain that IP address information." Ex. A, ¶ 25. However, neither statement by Agent Squire was sufficient to assure the Magistrate of the tip's reliability. Agent Squire did not state that the IP address information had reached the FLA through a reliable first-hand source rather than through multiple layers of hearsay. *Cf. Gates*, 462 U.S. at 234 (noting that the informant's "explicit and detailed description of alleged wrongdoing, along with a statement that the event was observed *first-hand*, entitles his tip to greater weight than might otherwise be the case"); *United States v. Taylor*, 985 F.2d 3, 5-6 (1st Cir. 1993) (noting that an affidavit may support an informant's veracity "through the very specificity and detail with which it relates the informant's *first-hand* description of the place to be searched or the items to be seized"). Nor did Agent Squire aver that *no* FLA had "interfered with, accessed, searched, or seized any data from any computer in the United States." Ex. A, ¶ 25. Instead, Agent Squire left the

Magistrate to guess at how the FLA had obtained the information and to merely ratify Agent Squire's conclusion that the tip was a reliable one.

The First Circuit has found that a lack of explanation of the basis of knowledge for an informant's tip undermines a finding of probable cause. *Gifford*, 727 F.3d at 99-101. In *Gifford*, an informant told the affiant that the defendant was growing marijuana at his house. *Id*. at 95. However, the affidavit included no information about the informant's basis of knowledge for the tip. It was therefore unclear "whether the informant just happened to view the grow operation, heard about it as hearsay, or had direct, first-hand knowledge of the grow operation in the Gifford home." *Id*. at 100. Because the affidavit lacked any "statements as to the informant basis of knowledge," there was no means for the magistrate to determine "whether that information was obtained first-hand or through rumor." *Id*. The lack of any information about the source of the informant's knowledge weighed against a reliability finding in *Gifford*.

The facts of this case mirror those in *Gifford* and compel the same conclusion. As in *Gifford*, it is entirely unclear how, when, and through what method the FLA that provided the tip learned about the IP address. Without that information, there was no basis for the magistrate to determine whether the content of the tip from the FLA was reliable and trustworthy. By not divulging any information about the FLA's basis of knowledge, the magistrate was left with no reason to believe that the tip was obtained through a reliable and trustworthy source or method. Simply repeating the FLA's allegation without further explaining how the FLA uncovered the connection between the IP address and the accessing of child sexual abuse material was insufficient to adequately establish the basis of knowledge of the tip. The first and second factors of *Tiem Trinh* – "whether the affidavit establishes the probable veracity and basis of knowledge of persons

supplying hearsay information" and "whether an informant's statements reflect first-hand knowledge" – therefore weigh in Mr. Bateman's favor. *Tiem Trinh*, 665 F.3d at 10.

ii. The Affidavit Reflects No Effort From Law Enforcement To Corroborate The Tip.

In addition to the lack of information about the basis of knowledge or reliability of the method used to obtain the IP address, the affidavit does not include any facts that actually or meaningfully corroborated the tip from the FLA that an internet user had "accessed online child sexual abuse and exploitation material via a website." Ex. A, ¶ 23. While Agent Squire did include a description of the steps U.S. law enforcement took to confirm who lived at [redacted], that investigation only corroborated the fact that someone lived at the physical address associated with the IP address identified by the FLA. None of that investigation corroborated the tip that that particular IP address was used to access child pornography on April 30, 2019.

In the affidavit, Agent Squire briefly detailed the steps agents took to identify who, if anyone, lived at [redacted]. They deduced, according to the affidavit, that Mr. Bateman owned a condominium at that address, that he listed [redacted] as his residential and mailing address at the RMV, and that he resided there with an adult woman. Ex. A, ¶ 27-30. One agent also saw cars that were registered to Mr. Bateman and the woman who resided there with him parked in front of the condo one day before the warrant was submitted to the Magistrate. *Id*. While this information certainly may have substantiated a claim that Mr. Bateman lived at that address in December 2019, none of it corroborated the allegation made by the FLA – that an internet user at [redacted] had accessed child sexual abuse material in April 2019. *See Gifford*, 727 F.3d at 99-102 (DMV records that confirmed the defendant lived at his address did not corroborate an informant's tip that there was an ongoing grow operation at that address). The third factor identified in *Tiem Trinh* – "whether some or all of the informant's factual statements were

corroborated wherever reasonable or practicable" – therefore weighs in favor of Mr. Bateman. *Tiem Trinh*, 665 F.3d at 10.

In sum, Agent Squire failed to establish the basis of knowledge for the tip or the reliability of the method used to obtain the information in the tip. Agent Squire also failed to include any facts that corroborated the unreliable tip. The information provided in the affidavit therefore did not create a "substantial basis" for the magistrate to conclude that probable cause existed. *Gates*, 462 U.S. at 238-39.

b. The Warrant Was Stale.

Stale information cannot establish probable cause that evidence of criminal activity will be found at the place searched. *United States v. Grubbs*, 547 U.S. 90, 96 n.2 (2006). Whether information is stale does not depend solely on the number of days between the events described in the affidavit and the issuance of the warrant. *Tiem Trinh*, 665 F.3d at 13–14. Courts look instead at a number of factors, including "the nature of the information, the nature and characteristics of the suspected criminal activity, and the likely endurance of the information." *Id.* (citing *United States v. Morales-Aldahondo*, 524 F.3d 115, 119 (1st Cir. 2008)). In cases involving child pornography, courts have often determined that the passage of a significant amount of time between the acquisition of the incriminating information and the obtaining of a warrant does not render the information stale where the magistrate was provided with information supporting a finding that such materials are likely to have been retained by their possessor. *See, e.g., Morales-Aldahondo*, 524 F.3d at 119.

Here, the FBI did not have probable cause to search Mr. Bateman's home in December 2019 when the alleged access to child sexual abuse material occurred in April 2019 – seven months earlier. The affidavit did not include any allegations specific to Mr. Bateman regarding any

propensity or habits of keeping a collection of child pornography. Moreover, the affidavit failed to state what exactly was accessed on the website, whether it was downloaded or saved in any manner, or whether there were multiple visits to the website – facts that could have bolstered probable cause. *See United States v. Raymonda*, 780 F.3d 105 (2d Cir. 2015) (no probable cause where the affidavit alleged that "on a single afternoon more than nine months earlier, a user with an IP address associated with Raymonda's home opened between one and three pages of a website housing thumbnail links to images of child pornography, but did not click on any thumbnails to view the full-sized files").

Without more information specific to Mr. Bateman, and without more information about the material allegedly viewed and the number of visits to the website, there was not probable cause to believe that Mr. Bateman's home contained evidence of a crime. The warrant was unlawfully issued, and all evidence obtained as a result of the search conducted pursuant to the warrant must be suppressed.

II. The Affiant Made Material Omissions and Misstatements and Mr. Bateman is Entitled to a *Franks* Hearing as a Result.

In *Franks v. Delaware*, the Supreme Court held that a defendant is entitled to a hearing to challenge the truthfulness of statements in a search warrant affidavit if he makes "a substantial preliminary showing" that the statements were "knowingly and intentionally [false], or [made] with reckless disregard for the truth," and that the falsehood was "necessary to the finding of probable cause." *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978). "An allegation is made with reckless disregard for the truth if the affiant in fact entertained serious doubts as to the truth of the allegations or where circumstances evinced obvious reasons to doubt the veracity of the allegations in the application." *Gifford*, 727 F.3d at 98 (internal quotations omitted). "Suppression of the evidence seized is justified if, at such a hearing, the defendant proves intentional or reckless

falsehood by preponderant evidence and the affidavit's creditworthy averments are insufficient to establish probable cause." *United States v. Tanguay*, 787 F.3d 44, 49 (1st Cir. 2015).

The right to a Franks hearing is triggered not only by false statements but also by material omissions. *Id.*; *United States v. Cartagena*, 593 F.3d 104, 112 (1st Cir. 2010). When a defendant alleges a material omission has been made, "[t]he required showing is two-fold: first, the omission must have been either intentional or reckless; and second, the omitted information, if incorporated into the affidavit, must be sufficient to vitiate probable cause." *Tanguay*, 787 F.3d at 49. The First Circuit has held that recklessness may be inferred where "the omitted information was critical to the probable cause determination." *Gifford*, 727 F.3d at 99-100.

Special Agent Squire made omissions and misstatements knowingly and intentionally, or with reckless disregard for the truth regarding three key issues. First, Agent Squire made material misstatements about the nature, origin, and reliability of the tip from the FLA. Second, Agent Squire made material omissions about the method(s) used by the FLA to identify the IP address. Third, Agent Squire misrepresented the relationship between U.S. law enforcement and the FLA in the affidavit. Each of these misstatements and misrepresentations went directly to the heart of the probable cause analysis. The magistrate would not have issued the warrant had these misrepresentations been corrected in the affidavit because the reformed affidavit would not establish probable cause. Mr. Bateman is therefore entitled to a *Franks* hearing.

a. Agent Squire Misrepresented the Nature, Origin, and Reliability of the Tip.

The affidavit relies entirely on Agent Squire's assertion that an FLA notified U.S. law enforcement that a particular IP address "was used to access online child sexual abuse and exploitation material via a website that the FLA named and described as Website A." Ex. A, ¶ 23. There is no other allegation of criminal activity anywhere in the affidavit. However, this fact is

inherently misleading and factually incorrect. Agent Squire did not repeat the tip from the [redacted] verbatim. Rather, he added language that misled the magistrate into believing that U.S. law enforcement had more evidence of criminal activity that it did.

The exact words of the tip from the [redacted] tip document were: "[redacted]" *See* [redacted] Intelligence Report (attached as Exhibit D). Agent Squire did not copy or repeat this language into the affidavit. Instead, he stated the following: "FLA had determined that on April 30, 2019 at 10:38:18 UTC, IP address 73.142.30.140 was used to access online child sexual abuse and exploitation material *via a website*. According to the FLA, the website had an explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on BDSM, hurtcore, gore, and death-related material including that of children. Users were required to create an account (username and password) in order to access the majority of the material." Ex. A, ¶ 23.

While this change appears slight, its significance in the affidavit was great. By manipulating the language of the tip, Agent Squire created the impression that the [redacted], and therefore U.S. law enforcement, had information that the IP address was used to visit Website A *and then used to access child sexual abuse material*. The implication in the affidavit is that the internet user associated with that IP address viewed or downloaded the child sexual abuse material available on Website A and that, because the majority of the material was only available through an account, the internet user had accessed the child sexual abuse material through that account.

However, this implication misrepresents the substance of the tip from the [redacted]. The [redacted] did not provide any such information, nor did U.S. law enforcement have any such evidence. Rather, the tip from the [redacted] conveyed only that the IP address in question was used to *access the website*.

The phrasing of the [redacted] Intelligence Report supports this interpretation of the tip. In the Intelligence Report, the [redacted] states that the IP address was used to "access online child sexual abuse and exploitation material, with an explicit focus on the facilitation of sharing child abuse material." Ex. D. The tip is inscrutable as it is written because it is unclear how "child sexual abuse and exploitation material" (i.e., videos and images) can have an "explicit focus" on the *facilitation of sharing the same material*. Its meaning only becomes clear if the phrase "online child sexual abuse and exploitation material" means Website A, rather than images or videos depicting child sexual abuse. In other words, the Intelligence Report should be read as "On 2019-04-30 10:38:18 UTC 73.142.30.140 was used to access [Website A], with an explicit focus on the facilitation of sharing child abuse material (images, links, and videos), emphasis on BDSM, hurtcore, gore and death-related material including that of children." This reading is consistent with, and tracks the exact language of, the [redacted] Intelligence Report identifying the website, which uses the identical language to describe the *website itself*, not the activity of the internet user. *See* Ex. F.[4]

Other parts of the affidavit reflect that this was, and has been, U.S. law enforcement's understanding of the [redacted] tip. *See* Ex. A at ¶ 24 ("I submit that the **website accessed by the IP address** 73.142.30.140 appears to be Website A."); ¶ 27 ("According to publicly available information, IP address 73.142.30.140 – the one used to **access Website A**… is owned/operated by Comcast."); ¶ 39 ("I am aware that this investigation revealed that an individual located at the

[4] The images and videos named in Ex. F appear to be those shared on the website, *not those accessed, viewed, or downloaded by any one user, let alone Mr. Bateman.*

address listed in Attachment A **accessed a website** that is dedicated to the sexual exploitation of children, and which is accessed through the Tor network.").

In rewording the tip from the [redacted], Agent Squire also omitted the crucial fact that the homepage of Website A did not contain any child sexual abuse material. Screenshots of the website provided by the government show that in order to "access" any child sexual abuse material, an individual would have to navigate past the homepage and, as Agent Squire acknowledges, log in with a username and password to access the material in question. Contrary to the impression created by Agent Squire in the affidavit, the [redacted] did not state in its tip that it had any information that the internet user associated with that IP address had an account on Website A, nor did it state that the user had logged into the website using a username and password.

The distinction between the substance of the tip and the retelling of that tip in the affidavit is important. There is a fundamental difference between: 1) evidence of a one-time visit to a website where no images, videos, or links to child pornography materials were either visible or available on the website's homepage, and no such items were viewed and/or downloaded and 2) evidence of an individual creating an account on that website and then using that account to view, download, or possess materials that would have only been accessible once a user navigated past the homepage. *See United States v. Falso*, 544 F.3d 110, 120-21 (2d Cir. 2008) (finding no probable cause for possession of child pornography when it was alleged that defendant "appear[ed]" to have "gained access or attempted to gain access" to the cpfreedom.com website—which did not require registering an account or logging in—and that even if one inferred that the defendant had accessed cpfreedom.com, there was no specific allegation that the defendant "accessed, viewed or downloaded child pornography"). The information the [redacted] relayed to U.S.

law enforcement fell squarely into the first category, which was insufficient to establish probable cause.

By manipulating the language in the tip from the [redacted], Agent Squire misrepresented the information available to U.S. law enforcement and created a misleading impression that U.S. law enforcement had more evidence of criminal activity than it actually did regarding the sole allegation of criminal activity in the affidavit. Agent Squire's misrepresentation about the nature of the tip was recklessly made and was "necessary to the finding of probable cause." *Franks*, 438 U.S. at 155-56. Had Agent Squire been truthful about the tip and stated that U.S. law enforcement had received information only that the IP address was used on a single occasion to visit a website where no child pornography was visible or available on the homepage, the magistrate could not have found sufficient probable cause to issue the warrant. Mr. Bateman is therefore entitled to a *Franks* hearing on these false statements.

In addition to this misrepresentation about the nature of the tip from the [redacted], Agent Squire also omitted important information about the origin and reliability of the tip. In the affidavit, Agent Squire made a number of representations about the FLA that had provided the tip (now known to be the [redacted]) and its reliability. Specifically, Agent Squire stated that that FLA (again, [redacted]) had "a history of providing reliable, accurate information in the past" and that it was "a national law enforcement agency of a country with an established rule of law." Ex. A, ¶ 23. Agent Squire averred that the FLA (the [redacted]) had obtained the information in the tip through an investigation that was "lawfully authorized in FLA's country pursuant to its national laws," and that the FLA (the [redacted]) had not "interfered with, accessed, searched, or seized any data from any computer in the United States in order to obtain the IP address information." *Id*. at ¶ 25. Finally, Agent Squire

claimed that prior tips from the FLA (the [redacted]) had led to an arrest, the rescue of children subject to abuse, and the seizure of evidence. *Id*. at ¶ 26.

However, Agent Squire omitted from the affidavit the fact that there was not just one FLA involved in the investigation of Website A, but two, from two entirely different countries. The [redacted], which provided the tip to U.S. law enforcement and which Agent Squire took pains to assure the court was subject to the rule of law, was seemingly not involved in the seizure of the website's server. Instead, the government recently disclosed that a second FLA – which it has refused to name – seized the server in a country distinct from [redacted] – a country which it has also refused to name. Additional information – such as who participated in the seizure and/or investigation/investigation steps and what investigative steps were undertaken by the seizing FLA alone or in conjunction with other countries and/or law enforcement, including the United States – remains unknown. What little *is* known about the second FLA is that it was local to the server host country.

Agent Squire made no distinction between the two FLAs in the affidavit and failed to inform the court that there was even a second FLA involved in the investigation. Instead, Agent Squire created the misimpression that the tip and the source of that tip both originated from the same, allegedly reliable FLA. This impression was both misleading and inaccurate. While Agent Squire made a number of claims in the affidavit about the reliability of the FLA, those statements applied *only* to the FLA that provided the tip to U.S. law enforcement (again, [redacted]). There are no facts in the affidavit that address or establish the reliability or trustworthiness of the FLA that seized the server. Agent Squire did not, for example, make any assurances that the FLA that seized the server had a "history of providing reliable, accurate information." Nor did Agent Squire aver that the second FLA was from a country with an "established rule of law." Ex. A, ¶ 25. Likewise,

there are no facts in the affidavit that establish that the FLA that seized the server did not conduct a search or seizure of any computer in the United States (e.g. performing a so-called "Network Investigative Technique" (NIT)).

This misinformation went to the heart of the probable cause analysis. The tip from the [redacted] was the only allegation of criminal activity in the entire affidavit. It was also the only piece of information that created a nexus between Mr. Bateman, his home, and the alleged criminal activity. The omitted fact that there was a second FLA involved in obtaining the IP address information "require[s] that [this Court] alter in significant ways the weight [it] give[s] to" the tip. *Gifford*, 727 F.3d at 101. Without assurances in the affidavit about the reliability and trustworthiness of the second FLA and the legality of its action, no Magistrate could find there was probable cause.

Because Agent Squire's misrepresentations and omissions regarding the nature, origin, and reliability of the tip were all "critical to the probable cause determination," this Court "may infer recklessness" on the part of Agent Squire. *Gifford*, 727 F.3d at 101. The reckless misrepresentations were "necessary to the finding of probable cause" and the omitted information, adding back into the affidavit, "is sufficient to vitiate probable cause." *Franks*, 438 U.S. at 155-56; *Tanguay*, 787 F.3d at 49. Mr. Bateman is therefore entitled to a *Franks* hearing.

b. The Affiant Made Material Omissions Regarding The Method Used by the FLA to Identify the IP Address.

In the affidavit, Agent Squire stated that the FLA ([redacted]) assured U.S. law enforcement that that FLA had not "interfered with, accessed, searched, or seized any data from any computer in the United States." Ex. A, ¶ 25. This assurance, combined with the omitted fact that there was more than one FLA involved in the investigation, created the impression that no law enforcement agency, anywhere, had "interfered with, accessed, searched, or seized" data from a computer in the United States. However, an expert declaration submitted in a case seemingly identical to Mr.

Bateman's, and arising out of the same tip, suggests that the specific IP address could not have been identified without running a NIT or, in the alternative, an error-prone and unreliable traffic analysis technique. *See* Declaration of Steven Murdoch at ¶ 22-32, *United States v. Sanders*, No. 20-cr-00143 (E.D. Va. Sept. 17, 2021), ECF No. 464-2 (attached as Exhibit H).

In Professor Murdoch's declaration, he explains that "there are only two techniques for identifying the IP address of a user using Tor Browser properly: traffic-analysis (which can generate errors) or a Network Investigative Technique (which interferes with a user computer)." Ex. H, ¶ 23. A NIT works "by forcing the user's computer to disclose its IP address by connecting directly to a law-enforcement server without using the Tor network." *Id*. at ¶ 27. A NIT "necessarily interferes with a user's computer wherever it is located." *Id*. at ¶ 32.

Traffic analysis, on the other hand, is a technique that attempts to "identify which user is communicating with which Onion Service by comparing patterns of when and how much data is sent (as opposed to looking at the content of the data, which is not visible to observers)." *Id*. at ¶ 17. Professor Murdoch states that before 2016, "traffic analysis on Tor was unreliable, but there were concerns that it might be possible in some cases." However, in 2016, Tor addressed this issue and introduced a new extension to its software that caused traffic analysis to "introduce more errors, both false positives (where a user is incorrectly identified as having visited the Onion Service) and false-negatives (where a user is incorrectly identified as not having visited the Onion Service)." *Id*. at ¶ 19. This measure, and others, have made it "even more difficult to use traffic-analysis to de-anonymize Tor users." *Id*. at ¶ 21.

The use of either technique by [redacted] or another FLA would significantly undermine the veracity of the affidavit and its probable cause showing. If traffic analysis was used to uncover the IP address, the undisclosed fact that the technique is inherently error-prone would significantly

undermine the strength and reliability of the tip from [redacted]. *See id*. at ¶ 22-32. No magistrate, had he or she been aware that this fundamentally unreliable technique was used to obtain the IP address, would find there was probable cause, especially where the tip about the IP address was not corroborated by any other facts.

Alternatively, the use of a NIT would reveal a substantial misrepresentation in the affidavit, which relies on Agent Squire's assurance that no computer in the United States had been searched. The deployment of a NIT is an unlawful warrantless search. *See United States v. Tagg*, 886 F.3d 579, 584 (6th Cir. 2018); *United States v. Anzalone*, 208 F. Supp. 3d 358, 366 (D. Mass. 2016), *aff'd*, 923 F.3d 1 (1st Cir. 2019). Had any law enforcement agency deployed a NIT to obtain the IP address without a warrant, the Magistrate could not have considered the results of that search in the probable cause analysis. *See United States v. Dessesaure*, 429 F.3d 359, 367 (1st Cir. 2005) ("[W]hen faced with a warrant containing information obtained pursuant to an illegal search, a reviewing court must excise the offending information and evaluate whether what remains is sufficient to establish probable cause.").

Agent Squire's omissions regarding the method used to obtain the IP address were material because if the omitted information – either that a NIT or an error-prone traffic analysis was used – was included in his affidavit, it would be "sufficient to vitiate probable cause." *Tanguay*, 787 F.3d at 49. This Court may infer that the information was omitted recklessly because the omitted information was "critical to the probable cause determination." *Gifford*, 727 F.3d at 99-100. Mr. Bateman is therefore entitled to a *Franks* hearing on this issue as well.

c. The Affiant Misrepresented The Nature Of The Relationship Between U.S. Law Enforcement And The FLAs And Omitted Facts That Would Have Revealed that the FLAs' Actions Were Subject to the Exclusionary Rule.

Agent Squire's final misrepresentations involved omitting facts about the role of U.S. law enforcement in the investigation of Website A. Specifically, Agent Squire withheld information that would have shown that 1) U.S. law enforcement was engaged in a "joint venture" with the FLAs and 2) the FLAs engaged in conduct that would shock the judicial conscience such that the FLAs' actions would be subject to the exclusionary rule.

Generally, "the Fourth Amendment's exclusionary rule does not apply to foreign searches and seizures." *United States v. Valdivia*, 680 F.3d 33, 51 (1st Cir. 2012). There are, however, two exceptions to that rule: "(1) where the conduct of foreign police shocks the judicial conscience, or (2) where American agents participated in the foreign search, or the foreign officers acted as agents for their American counterparts." *Id*. Here, both exceptions would apply to the conduct of the FLAs. Running a NIT to obtain an IP address of a computer in the U.S. – conduct that is unlawful in the U.S. without first obtaining a warrant – and then hiding that information from a magistrate judge would "shock the judicial conscience." *Id*. Likewise, the information available to the defense suggests that there was a "joint venture" afoot between the United States and the FLAs such that the exclusionary rule would apply to one (or both) of the FLAs running a NIT on a computer in the United States. *See id*. However, Agent Squire minimized the collaborative relationship between the agencies and withheld facts that would have established that "American agents participated in the foreign search, or the foreign officers acted as agents for their American counterparts." *Id*.

[redacted]

[redacted][5] [redacted]

[redacted]

[redacted]

[redacted][6] [redacted]

[redacted]

[redacted]

[redacted]

[redacted][7] [redacted]

[redacted]"[8] [redacted]

[redacted].[9]

Although the Affidavit indicates that "U.S. law enforcement personnel did not participate in the investigative *work* through which [redacted] identified the IP address information provided by

[5] *See* [redacted]

[6] *See* [redacted]

[7] *See* [redacted]

[8] *Id.*

[9] *See* [redacted]

[ ],” Ex. A, ¶ 25, the ’s own representations about its collaborative work through its international liaison officers belie any conclusion that they solely engage in a simple information-sharing relationship with other countries. Specifically,

[10]

Cases filed in this district and others demonstrate that the tips provided by to U.S. law enforcement are more than just an informal, one-off relaying of information. *See, e.g., United States v. Kiejzo*, No. 1:20-cr-40036-TSH (D. Mass.); *United States v. Corwin*, No. 2:21-cr-00218-JS (E.D.N.Y.), D.E. 1 (unsealed at D.E. 4) (complaint affidavit indicates that in August 2019, the FBI received information from an FLA regarding an IP address which allegedly accessed on April 27, 2019); *United States v. Sanders*, No. 1:20-cr-00143-TSE (E.D. Va.).

”[11]

[10]

[11] *Id*.

[redacted][12] [redacted]

[redacted][13]

[redacted]

[redacted]"[14] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]"[15]

The link between the U.S. and [redacted] in these kinds of operations is neither nebulous nor abstract – indeed, Agent Squire asserted that he was an "active member of a multinational, multi-agency working group that coordinates national and international operations to combat child exploitation on the dark web[.]" Ex. A, ¶ 1. The government, in a discovery response,

[12] *Id*.

[13] *Id*.

[14] See Twitter profile [redacted] and attached screenshots at Exhibit I.

[15] *See* "Justice News: Deputy Assistant Attorney General Richard W. Downing Delivers Remarks at the Academy of European Law Conference on "Prospects for Transatlantic Cooperation on the Transfer of Electronic Evidence to Promote Public Safety," April 5, 2019 (emphasis added), available at: https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-richard-w-downing-delivers-remarks-academy-european-law (last accessed Dec. 10, 2021).

acknowledged that "there is at least one representative of the FLA in the working group." *See* Exhibit A to Defendant's Motion to Compel filed under seal at D.E. 76.

Based on the materials available to the defense, it appears there was, at the minimum, a significant collaboration between the United States and the [redacted]. By withholding this information from the affidavit, Agent Squire obscured the extent to which there was a "joint venture" between the two law enforcement agencies such that the actions taken by the [redacted] would be subject to the exclusionary rule. This information was material as the tip from the [redacted] formed the entire basis for probable cause in the affidavit. Mr. Bateman is therefore entitled to a *Franks* hearing on this misrepresentation.

Because the government has not disclosed the identity of the second FLA, the defense has been unable to investigate the possibility of a joint venture or cooperation between the United States and the second FLA. However, a recent case from the Northern District of Illinois, *United States v. Mitrovich*, 458 F. Supp. 3d 961 (N.D. Ill. 2020), sheds light on how U.S. law enforcement engages in these very kind of joint investigations of hidden services websites on Tor with FLAs and how that might have occurred in this case. In *Mitrovich*, the FBI began investigating a child pornography website in 2014. *Id*. at 963. Sometime that year, the FBI "obtained the ability to identify IP addresses associated" with the website, and learned that the website was hosted in the Netherlands, with the head administrator residing in Australia. *Id*. After the FBI shared that information with Australia, law enforcement agencies from Australia and New Zealand seized control of the website, operated it undercover, and shared backup copies of the website with the FBI. *Id*. As part of its investigation, the Australian and New Zealand authorities uploaded a hyperlink onto the website that, when clicked, allowed them to capture the clicker's IP address, which would have otherwise been concealed by Tor. *Id*. One particular user – known as

"cyberguy" – clicked on the hyperlink, thereby revealing his IP address, which was located in the United States, to the Australian and New Zealand authorities. *Id*. Australia and New Zealand sent the IP address to the FBI, which then obtained records from Comcast to identify the physical address associated with the IP address. *Id*. The FBI subsequently obtained a search warrant for that address – the defendant's home – and discovered child pornography materials therein. *Id*.

The facts in *Mitrovich* demonstrate how a U.S. law enforcement agency could *and did* participate in the seizure of a website server with an FLA. The facts also demonstrate that while U.S. agents may not necessarily direct an investigation into one particular IP address, a U.S. law enforcement agency could be engaged in a joint venture to uncover IP addresses within the United States. In *Mitrovich*, the court held that the defendant had made a *prima facie* showing that a Fourth Amendment search had taken place and that U.S. law enforcement was sufficiently involved to implicate the exclusionary rule such that the defendant was entitled to discovery on the issue. *Id*. at 967. Here, Mr. Bateman has made a substantial preliminary showing that Agent Squire omitted crucial information about the existence of a second FLA involved in the investigation of Website A. He has demonstrated that there was a joint venture between U.S. law enforcement and the [redacted], the only FLA so far identified by the government. The omissions and misrepresentations about the investigation into Website A by multiple FLAs and the relationship between those FLAs were material to probable cause and Mr. Bateman is entitled to a *Franks* hearing as a result.

CONCLUSION

For the above reasons, this Court should suppress all evidence and illegal fruits obtained pursuant to the invalid search warrant and grant Mr. Bateman a *Franks* hearing.

Respectfully submitted,
PAUL BATEMAN
By His Attorney,

/s/ Sandra Gant
Sandra Gant, BBO # 680122
Federal Public Defender Office
51 Sleeper Street, 5th Floor
Boston, MA 02210
Tel: 617-223-8061

/s/ Caitlin Jones
Caitlin Jones, MN ID # 0397519
Federal Public Defender Office
51 Sleeper Street, 5th Floor
Boston, MA 02210
Tel: 617-223-8061

CERTIFICATE OF SERVICE

I, Sandra Gant, hereby certify that this document filed through the ECF system will be sent electronically to the registered participant(s) as identified on the Notice of Electronic Filing (NEF) on December 27, 2021.

/s/ Sandra Gant
Sandra Gant